UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 19-CR-02

ALEXANDER P. BEBRIS,

Defendant.

DECISION AND ORDER DENYING MOTION TO SUPPRESS

On January 15, 2019, a grand jury sitting in Milwaukee returned an Indictment charging Defendant Alexander P. Bebris with Distribution of Child Pornography in violation of 18 U.S.C. § 2252A(a)(2)(A) and Possession of Child Pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). The charges stem from Facebook's discovery that Bebris uploaded several child pornography images via Facebook Messenger in September 2018. Facebook relayed that information to the National Center for Missing and Exploited Children (NCMEC), which then sent it to local law enforcement in Wisconsin. In December 2018, the Winnebago County Sheriff's Office (WCSO) obtained and executed a search warrant at Bebris' residence based on the information provided by NCMEC, where officers found additional child pornography files.

Currently before the court is Bebris' motion to suppress the evidence and statements obtained following the search of his residence. Bebris claims that his Fourth Amendment rights were violated when private entities and law enforcement reviewed the illegal images he allegedly uploaded to Facebook. More specifically, Bebris contends that Facebook and NCMEC were acting as agents of the Government when they identified and reviewed the child pornography files

Bebris allegedly uploaded to Facebook and forwarded the information concerning the uploads to WCSO. An evidentiary hearing was held on Bebris' motion on December 3, 2019, and the parties submitted both pre-hearing and post-hearing briefs. In addition, the court heard argument and reviewed briefing on Facebook's motion to quash the subpoena that Bebris' attorneys issued to it. For the reasons that follow, Bebris' motion to suppress will be denied and Facebook's motion to quash will be granted.

FINDINGS AND ANALYSIS

A. Expectation of Privacy

The evidentiary hearing and most of the argument and briefing centered on the issue of whether Facebook and NCMEC act as government agents in the investigation of child pornography. The more immediate question, however, is whether Bebris had a reasonable expectation of privacy in the Facebook messages he sent containing child pornography. I conclude he did not.

"[T]he application of the Fourth Amendment depends on whether the person invoking its protection can claim a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by government action." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (internal quotations omitted). "A defendant seeking to suppress the fruits of a search bears the burden of demonstrating both that he held an actual subjective expectation of privacy and that the expectation 'is one that society is prepared to recognize as reasonable.'" *United States v. Villegas*, 495 F.3d 761, 767 (7th Cir. 2007) (quoting *United States v. Yang*, 478 F.3d 832, 835 (7th Cir. 2007)). While it appears clear, assuming the allegations in the Indictment are true, that Bebris had a subjective expectation of privacy in his Facebook email containing child pornography, i.e., he didn't think he'd be caught, his expectation was not objectively reasonable in light of

Facebook's published Community Standards and the terms of service he agreed to as a condition of opening a Facebook account.

Facebook is a well-known media company and electronic service provider ("ESP"). Facebook users create user names and can communicate with other Facebook users through, among other things, Facebook Messenger. Facebook has a corporate policy that prohibits content that sexually exploits or endangers children. *Community Standards, Section 7: Child Nudity and Sexual Exploitation of Children*, FACEBOOK, https://www.facebook.com/communitystandards/safety (last visited Mar. 5, 2020). The policy expressly warns users: "When we become aware of apparent child exploitation, we report it to the National Center for Missing and Exploited Children (NCMEC), in compliance with applicable law." *Id.*, Decl. of Michael Francis Xavier Gillin, II, ¶ 3, Dkt. No. 41 at 5. Facebook also discloses to its users that it collects data about "the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others." *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/update#legal-requests-prevent-harm (last visited Mar. 5, 2020). Users are told this information is used, inter alia, to "promote safety and security on and off of Facebook Products." *Id.* Among the third parties with whom users are told Facebook shares such information are law enforcement agencies. Facebook explains that "we access, preserve and share your information with regulators, law enforcement or others . . . [w]hen we have a good-faith belief it is necessary to: detect, prevent or address . . . harmful or illegal activity." *Id.*

In the face of these disclosures, any expectation of privacy Bebris had with respect to child pornography uploaded via his Facebook Messenger account would be objectively unreasonable. *See United States v. Wilson*, No. 3:15-cr-02838-GPC, 2017 WL 2733879, at *7 (S.D. Cal. June

26, 2017) ("This express monitoring policy regarding illegal content, which Defendant agreed to, rendered Defendant's subjective expectation of privacy in the four uploaded child pornography attachments objectively unreasonable."); *United States v. Ackerman*, 296 F. Supp. 3d 1267, 1273 (D. Kan. 2017) ("In this case, AOL's TOS [terms of service] similarly limits Defendant's objectively reasonable expectation of privacy. As noted above, the TOS informed Defendant that he must comply with applicable laws and that he could not participate in illegal activities. AOL's TOS also informed Defendant that if he participated in illegal activities or did not comply with AOL's TOS, it could take technical, legal, or other actions without notice to him. Thus, the Court concludes that Defendant cannot establish a reasonably objective expectation of privacy in this particular email and its four attachments (containing child pornography) after AOL terminated his account for violating its TOS."); *United States v. Stratton*, 229 F. Supp. 3d 1230, 1242 (D. Kan. 2017) ("[B]ecause the Terms of Service Agreement reduced defendant's reasonable expectation of privacy in the information stored on his PS3 device, the court finds that the Fourth Amendment does not apply to Sony's search of defendant's images.").

This is not to say that, as a general matter, an individual's expectation of privacy in his or her own email account is not reasonable. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) ("[W]e hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP.") (internal quotations omitted). In *Warshak*, the government used the Stored Communications Act (SCA), 18 U.S.C. §§ 2701 *et seq.*, to compel an internet service provider (ISP) to disclose 27,000 of the defendant's private emails in the course of its investigation of a scheme to defraud predicated on the sale of an herbal supplement purported to enhance male sexual performance. Although some of the emails were incriminating, there was no allegation that they contained contraband. Moreover, the

disclosure of the emails in *Warshak* was compelled by the government; it was not initiated by the ISP for its own purposes and in compliance with its terms of use. Based on these facts, the court concluded that the government's conduct violated the defendant's Fourth Amendment rights. But neither *Warshak*, nor any of the other cases cited by Bebris, have held that one's expectation of privacy in child pornography sent via email is reasonable in light of the express disclosure by the ESP that such content is not allowed and will be reported to law enforcement. Such an expectation is not "one that society is prepared to recognize as reasonable." *Katz v. United States*, 389 U.S. 347, 361 (1967).

B. Facebook as Government Agent

Even if his expectation of privacy was reasonable, Bebris' motion would nevertheless fail because Facebook is not a government agent, and thus its actions in detecting the child pornography and sending the CyberTipline Reports to NCMEC were private actions not attributable to the government, regardless of whether NCMEC is a government agent or not. The Fourth Amendment's purpose is to protect citizens against unreasonable searches and seizures by the government. It does not apply to searches or seizures performed by private individuals or entities unless they are acting as an instrument or agent of the government. In order to determine whether an individual was acting as a private party or as an "instrument or agent" of the government, courts look to "whether the government knew of and acquiesced in the intrusive conduct and whether the private party's purpose in conducting the search was to assist law enforcement agents or to further its own ends." *United States v. Ginglen*, 467 F.3d 1071, 1074 (7th Cir. 2006) (internal quotations omitted). "Other useful criteria are whether the private actor acted at the request of the government and whether the government offered the private actor a reward." *Id.*

Here, the government neither knew of nor acquiesced in Facebook's monitoring of Bebris' emails. No law enforcement agency was investigating Bebris until NCMEC alerted WCSO that child pornography had been uploaded using his account. Of course, law enforcement is aware that Facebook and other ESPs monitor the content of messages sent using their products, just like it knows private mail carriers monitor packages for drugs, but this does not make ESPs or private carriers agents of the government. *See United States v. Koenig*, 856 F.2d 843, 850 (7th Cir. 1988) (holding that employee of Federal Express was not acting as a de facto government agent when he opened suspicious package and discovered cocaine, notwithstanding carrier's historical maintenance of good relations with law enforcement officials and employee's past cooperation with such officials, where employee was following carrier's own policy authorizing search of suspicious packages for protection of itself and employees).

Facebook, like other ESPs have strong moral and business reasons of their own to prevent their products from being used to traffic in child pornography. No sane person, let alone a business that values its image and reputation, wants to be publicly associated with the sexual exploitation of children. As Facebook's Project Manager for Safety on its Community Operations team states in his declaration, "Facebook has an independent business purpose in keeping its platform safe and free from harmful content and conduct, including content and conduct that sexually exploits children." Gillin Decl. ¶ 3.

Other courts have recognized that other ESPs, like Facebook, have their own interest in preventing the use of their products to traffic in child pornography and that laws mandating the reporting of child pornography to law enforcement do not transform them into government agents. *See, e.g., United States v. Richardson*, 607 F.3d 357, 367 (4th Cir. 2010) ("We conclude that the statutory provision pursuant to which AOL reported Richardson's activities did not effectively

convert AOL into an agent of the Government for Fourth Amendment purposes."); *United States v. Cameron*, 699 F.3d 621, 638 (1st Cir. 2012) ("[I]t is certainly the case that combating child pornography is a government interest. However, this does not mean that Yahoo! cannot voluntarily choose to have the same interest."); *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013) ("A reporting requirement, standing alone, does not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography."). As one court recently noted, "district and circuit courts around the country . . . have universally rejected the arguments like Defendant's [that ESPs were acting as agents or instruments of the government in monitoring the email content of users and reporting suspected child pornography to NCMEC]." *United States v. Wolfenbarger*, Case No. 16-CR-00519-LHK-1, 2019 WL 6716357, at *12 (N.D. Cal. Dec. 10, 2019).

Bebris nevertheless argues that Facebook's cooperation with NCMEC, which is itself, in his view, an agent of the government, makes Facebook an agent of the government. He challenges the declarations filed by Facebook in support of its motion to quash the subpoena issued to compel its attendance at the evidentiary hearing held by the court and argues that he is entitled to live testimony, either in court or by video, to establish the close relationship between them.

To the extent Bebris' objection is to the admissibility of the declarations Facebook submitted, the objection is overruled. Bebris cites his Sixth Amendment right to compulsory process, but compulsory process is a trial right. It does not apply to pretrial proceedings. *Linder v. United States*, 937 F.3d 1087, 1090 (7th Cir. 2019) ("Compulsory process is a trial right; the Constitution does not entitle a criminal defendant to interview potential witnesses or take their depositions before trial."). Moreover, the Federal Rules of Evidence do not apply in full force to suppression hearings. Fed. R. Evid. 104(a), 1101(d)(1); *see United States v. Watson*, 87 F.3d 927,

930 (7th Cir. 1996) (holding that, "aside from privilege, exclusionary rules should not apply in a proceeding in which the court itself is considering the admissibility of evidence," including during suppression hearings) (citing *United States v. Matlock*, 415 U.S. 164, 173 (1974)); *see also United States v. Ozuna*, 561 F.3d 728, 736–37 (7th Cir. 2009) ("[T]he Rules of Evidence do not apply at pre-trial admissibility hearings. Rule 104(a) makes this explicit." (citations omitted)). As a result, Gillin's declarations are not excluded from consideration as inadmissible hearsay. The Court may receive the evidence and give it whatever weight it deserves. *Matlock*, 415 U.S. at 175.

To the extent Bebris' objection is that Facebook's declarations are not sufficient, the court concludes otherwise. Bebris' argument that NCMEC exceeded the scope of the private search conducted by Facebook is sufficiently addressed by Gillin's declaration describing the CyberTipline reports. Although the child pornography was originally identified by PhotoDNA, the computer program developed by Microsoft that allows ESPs, like Facebook, to more readily detect child pornography, the images were viewed by a person before they were submitted to NCMEC, as reflected in the reports themselves. Supp. Decl. of Michael Francis Xavier Gillin, II, ¶ 7, Dkt. No. 53 at 5. This evidence refutes Bebris' argument that NCMEC expanded Facebook's search.

But even if no Facebook employee had viewed the files, the result would be the same. As the Fifth Circuit noted in *United States v. Reddick*, Microsoft's PhotoDNA relies on hash-values to identify child pornography, and "hash value comparison allows law enforcement to identify child pornography with almost absolute certainty, since hash values are specific to the makeup of a particular image's data." 900 F.3d 636, 639 (5th Cir. 2018) (internal quotations omitted). Thus, opening the files identified as child pornography by comparison of hash values would not be a

significant expansion of a search previously conducted by a private party such that it would constitute a separate search. *Id.*

Bebris' further argument that direct testimony by a Facebook executive is needed to determine the level of cooperation between Facebook and NCMEC is likewise unconvincing. Even if Facebook did receive training from NCMEC on the use of PhotoDNA and the process of filing CyberTipline reports so that it could more effectively monitor its products for child pornography and assist law enforcement, this would not transform Facebook into a government agent or instrumentality. *See Koenig*, 856 F.2d at 849 ("And the fact that the DEA may have aided Federal Express in the development of a drug shipper profile does not establish that Federal Express would use the profile at the government's behest, rather than for its own, private purposes. Presumably Federal Express would desire the best profile it could obtain, the better to stem the tide of drugs shipped through its facilities. Use of an effective drug shipper profile, whatever its source, is consistent with a private business interest in protecting employees from contact with drug shipments.").

CONCLUSION

For these reasons, I conclude that Facebook's motion to quash Bebris' subpoena [Dkt. No. 40] should be granted. I further conclude from the evidence before me that Facebook was not acting as an agent or instrumentality of the government when it sent the CyberTipline reports to NCMEC identifying child pornography uploaded by Bebris' account via Facebook Messenger. And because Facebook acted independently, the court need not decide whether NCMEC is an agent of the government. Both because Bebris had no reasonable expectation of privacy in the child pornography depictions unloaded on his account and because Facebook was not acting as an agent of the government, his motion to suppress [Dkt. No. 28] is denied. The Clerk is directed

to place this matter on the court's calendar for a telephone conference with counsel to discuss further proceedings and, if necessary, schedule the matter for final pretrial and trial.

SO ORDERED at Green Bay, Wisconsin this 9th day of March, 2020.

s/ William C. Griesbach
William C. Griesbach, District Judge
United States District Court